IDNewswire
Trends in Personal Identification and Biometrics

www.cardtechnology.com Vol. 2 No. 14 July 9, 2003

NIST Fingerprint Test Announced Pg. 5
The National Institute of Standards and Technology will be conducting the Fingerprint Vendor Technology Evaluation this fall to test fingerprint systems and different scenarios.

Consumer Purchase Privacy Protection Pg. 5
Some 33.4 million Americans have purchased products to avoid identity theft and other types of fraud.

Biometric Enrollment Errors A Problem, But Not Fatal

When a credit card terminal doesn't read the magnetic stripe on the back of a card, it's a hassle. But there is a backup plan if this happens: the clerk manually enters the card number and other information into the machine.

It's potentially more serious if you are unable to enroll in a system that identifies you by a biometric, a physical characteristic such as your fingerprint, iris or face. That could mean you would not be able to use an automated system for entering a secure area. And for the company or government agency limiting access to that area, a system that fails to enroll many individuals could lead to compromised security or more expense in developing alternate means of authenticating identities.

Failure to enroll rates, or FTEs, are problems with all types of biometric systems. But they can be minimized by controlling lighting and other environmental factors at enrollment, and by figuring out good ways to train staff and the individuals enrolling in the system.

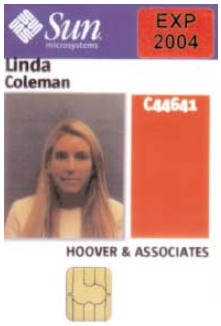
Nonetheless, expert say, enrollment failures will never entirely disappear. "FTE is an important, but often overlooked, metric when evaluating how biometric systems will perform in the real world," says Trevor Prout, director of marketing at the New York-based International Biometric Group. "In IBG's Comparative Biometric Testing, we have tested systems that had FTE rates as high as the low double-digits."

Fingerprints, probably the most deployed and researched biometric, will be used by the U.S. Department of Homeland Security for the US VISIT program to be launched early next year, which will track visitors to the U.S. from countries whose citizens must obtain visas to enter the United States.

The problem is fingerprints have anywhere from a 1% to 2% failure to enroll rate. "The best people are getting a 1.5% failure to enroll rate," says Charlie Wilson, manager of the imaging group in the information access division at the National Institute of Standards

> Enrollment, Page 2

Sun Shines A Spotlight On Smart Card IDs



You better have the backing of top management if you're going to change how everyone in a big corporation gets in the door and uses their computer. That was no problem at Sun Microsystems, where the introduction of smart card IDs is part of a broader initiative to enable Sun's 35,000 employees to work from anywhere. That top-level support may account for Sun's success in rolling out one of the most ambitious smart card-based employee IDs.

The mobile-workforce project is called iWork and has the enthusiastic backing of Sun's founder, chairman and CEO, Scott McNealy. While some Sun employees still have permanent offices, many share offices, reserving space as they need it.

In a recent article, McNealy estimated that Sun already is saving $50 million a year in reduced real estate and other operating expenses, and believes iWork ultimately will boost the computer maker's bottom line by $140 million annually.

Part of making this work, McNealy explained, was Sun's decision a few years back to abandon the traditional personal computer. Instead, all of a user's data and applications are stored on the network and employ-

> Sun, Page 4

Homeland Security Seeks Vendor Input On US VISIT

Further details about the U.S. Department of Homeland Security's plans to deploy biometrics at border crossings by the first of the year were revealed at an industry conference yesterday in Arlington, Va.

The US VISIT program, which will capture fingerprints and photographs of travelers from countries whose citizens require visas, is scheduled to be deployed at airports by Jan. 1, with biometrics at every seaport and land border crossing by the end of 2005.

During the meeting yesterday a timeline for US VISIT was discussed, and Homeland Security officials outlined plans to meet with vendors in hopes of developing a contract proposal that is feasible, given the tight deadlines for the project, according to vendors and consultants who attended the meeting.

Officials outlined a two-phase approach for equipping U.S. border crossings to check the biometric data of individuals entering the country on visas.

The system that will be put in place at airports by Jan. 1 will bulk up the existing IDENT system, or be "IDENT on steroids," as one consultant put it. IDENT is the two-fingerprint AFIS program used by the Bureau of Immigration

> US VISIT, Page 5

Smart Cards And Privacy

Gilles Lisimaque of Gemplus explains how smart cards can be used as a privacy-enabling technology.

> Smart Card Alliance, Page 6

Virginia County Uses Hand Biometrics

Chesterfield County in Virginia has installed IR Recognition Systems' HandReader for employees to access the county administration building during off-hours.

> Hand, Page 5

> Enrollment, Page 1

and Technology, a research arm of the U.S. Commerce Department.

Certain types of individuals typically have problems enrolling in fingerprint systems. "The conventional wisdom is that 1% to 2% of the population will not be able to enroll because they do not have sufficiently good quality fingerprints because they have worked with chemicals or have damaged their fingerprints over years of manual labor," says Prout.

Individuals with dry skin can pose a problem as well, Wilson says. Toronto-based Bioscrypt Inc. has an installation at a wood door factory, says Julia Webb, vice president of global sales and marketing at the fingerprint vendor. Working with wood dries out the skin on fingers, making it difficult for those workers to use the system, she says.

A far more ideal setting for fingerprints is at a New York financial services company where Bioscrypt also has installed its technology, she says. Bioscrypt enrolled 2,000 employees and had one FTE, or a .05% error rate.

The .05% is more typical of Bioscrypt's real-world FTE rates, Webb says. "Nobody out there has a perfect system," she says.

Prout says IBG's tests have validated the 1% to 2% FTE rates, with some systems performing better, and some worse. Tests have also shown a trade-off between failure to enroll rates and false rejection rates for individuals with poor quality prints, he says. "Some systems will enroll subjects with very poor quality prints, only to fail to recognize them later, while other systems will not enroll them in the first place," he says.

Proper training of how to use the scanners and care of equipment could reduce enrollment problems, Wilson says. "People have to be trained to use the equipment and keep it clean," he says. If those enrolling individuals place the finger squarely on the scanner, it will likely lead to lower enrollment errors.

Facial recognition is another biometric that will be widely deployed in the coming years, as travel documents store digital images of the document holder, and the United States begins capturing photographs of travelers for US VISIT.

It may seem unlikely that there would be FTEs with face because anyone can be photographed, but there are still problems, says NIST's Wilson. "You can always take a picture, but you can't always use it," he says.

A poor quality photo might not directly lead to an individual not being enrolled. But it's unlikely the facial recognition system would correctly identify that individual in the future, Wilson says.

The lighting for photos poses the biggest dilemma for facial biometrics, Wilson says. "If you do controlled illumination, you have a 90% correct verification rate," he says. "If you don't control your illumination, you won't get as good results, around 50%."

There is also the question of how many reference points can be taken from a face. Facial recognition works by taking a photograph and mapping out certain points and measuring the distance between them. Some individuals may have more or fewer points on their face to check depending on the quality of the photos.

'The conventional wisdom is that 1% to 2% of the population will not be able to enroll because they do not have sufficiently good quality fingerprints because they have worked with chemicals or have damaged their fingerprints over years of manual labor.'

– Trevor Prout, International Biometric Group

The International Civil Aviation Organization is constructing strict photo guidelines for travel documents for this reason, according to documents from the organization. In May, ICAO recommended that the document holder's photo be stored on a contactless smart card chip that will be embedded into passports. The organization is coming up with guidelines on how photos should be taken, such as how far away the individual should be from the camera, proper lighting, and other details, according to ICAO documents. *(See chart, page 3)*.

Although no one biometric can work for everyone, facial recognition is one of the more universal biometrics, says Frances Zelazny, director of communications at the Minnetonka, Minn.-based face and finger vendor Identix.

IBG's Prout has heard it said that individuals with dark facial features tend to have difficulty enrolling in a facial system, although he was not aware of any data documenting this. Zelazny says proper lighting can fix that problem. "As long as there is sufficient contrast, the LFA (local features analysis) algorithm will work," she says. Identix's LFA algorithm looks for 80 landmarks on an individual's face and then measures the difference between 14 and 23 of them for identification or verification.

Moorestown, N.J.-based Iridian Technologies Inc., the patent holder on iris recognition technology, is currently analyzing data on enrollment errors with its biometric, says James Cambier, vice president of engineering and chief technology officer at Iridian.

Most of the data for this test comes from a project Iridian is involved with in Afghanistan. Since March, a United Nations agency has been using iris recognition to process Afghan refugees who wish to repatriate to their country and receive an aid package. The UN has been using the system to prevent individuals from receiving multiple aid packages. These packages include a travel grant, food and other assistance.

Some 25,000 refugees have been enrolled in the system, with 100,000 enrollees expected before the end of the year, Cambier says. So far, the failure to enroll rate has been an unusually high .78%.

Initially, it looks as though eye injuries and disease might be for the cause of many of the enrollment errors, Cambier says. "There's an unusually high occurrence of eye disease and injury," he says. "You wouldn't normally expect to see that amount."

Iridian plans to examine the data to see if it needs to modify its technology in any way,

> Enrollment, Page 3

Environmental Issues Affecting Biometric Enrollment

– Lighting
– Trained personnel
– Proper equipment use
– Equipment cleanliness

> Enrollment, Page 2

Cambier says.

The enrollment environment and training also play a part in having the system work properly, Cambier says. "The key is to provide effective user feedback so they can properly position themselves and be prompted to keep the eye wide open," Cambier says.

At Schiphol Airport near Amsterdam, about one out of 10 individuals initially was rejected by the iris recognition system that provided an identifying biometric for the Privium card, which travelers use to more quickly pass border control at the airport. After training applicants to try out the system a few times so they look correctly into the image-capture device, which is like looking into a mirror with a frame in the center, the enrollment-failure rate dropped to around 1%, say officials at CMG, the Netherlands-based system integrator that implemented the voluntary smart card project.

As with facial, lighting can also play a factor in proper enrollment. "The best environment for enrollment is an office environment or any reasonable indoor environment," Cambier says. "As long as you don't have direct sunlight or bright reflections."

Since every biometric experiences some sort of FTE, organizations need to develop ways for individuals to gain access, even if they can't enroll. Angela Sasse, a professor of human-centred technology at University College London, says the solution is more than one biometric.

Identix's Zelazny has seen companies deploy multi-modal biometrics in some cases. Because there was some difficulty enrolling elderly or blue-collar workers in fingerprint systems, the Israeli government went with face and hand for one of the country's access control systems.

Biometrics isn't completely necessary for a fallback system, though, says Tony Mansfield, with the UK's National Physical Laboratory, a government-sponsored technology testing facility. "You need a robust secondary system that will handle people that are not able to enroll," he says.

As an example, when individuals have difficulty enrolling in a Bioscrypt system, the vendor lowers the security threshold for that individual, Webb says. The individual will identify themself with a PIN or token such as a smart card and then present the biometric. By lowering the threshold it allows the individual to be more easily recognized by the system, Webb says. "Usually we are able to get some sort of image," she says. <

ICAO Facial Recognition Photo Guidelines

Documents from ICAO show how photographs for travel documents should not be too close, or far away, with the last picture showing the preferred distance.

Lighting can play an issue with photos used for facial recognition. The first shot is too dark, while the second has too much light. The last photo shows the proper lighting.

Source: ICAO

> Sun, Page 1

ees access it from simple workstations by inserting their smart card into a reader built into the machine.

"One of the key enabling technologies of iWork are 'thin-client' computers (think keyboard, mouse and monitor), which make it possible for workers to simply insert a smart card and bring up their personal desktop, exactly as they left it, even on a different machine," McNealy wrote. "As a result, even most mobile workers are free from lugging around one of those expensive easily-stolen notebook computers – the network is their computer."

To accomplish this, Sun has deployed some 25,000 of its own Sun Ray thin-client computers around its 300 buildings in 100 countries. The original smart card Sun issued served that purpose alone. Now, the company is issuing a more ambitious smart card to its employees and several thousand vendors and temporary contract workers.

The new JavaBadge was designed to replace five different cards, badges and tokens that Sun was issuing, says Chris Saleh, JavaBadge project manager. These include the standard photo ID badge Sun employees must wear at work, the Sun Ray access card, an electronic purse card for 1,000 employees in the United Kingdom for paying at company cafeterias, an RSA SecurID token that mobile workers use to remotely access Sun's network, and a card to carry digital credentials as part of Sun's PKI system.

"We had five individual pockets of people going through the process of issuing cards to employees," Saleh says. "We said we could do all of this on a Java Card."

Java card is an operating system for smart cards. And not coincidentally, is Sun technology, a lightweight version of Sun's Java programming environment widely used for network-based applications. "We have a very aggressive Sun on Sun program where we deploy our own technology to drive competitive advantage and show customers the way," Saleh says.

Even with Java Card expertise and top-level support, rolling out a multifunction smart card has not been easy. The original systems integrator on the project, U.S. banking giant Citibank, dropped out after deciding that it did not want to be in the business of deploying ID cards for corporate customers. Sun then turned to smart card vendor Schlumberger for cards and some integration work, and to Activcard for developing applets for the smart cards and middleware that enables the cards to communicate with applications.

The fall of the high-tech economy led Sun to roll out the new smart card in two phases, rather than implementing all features at once, as initially planned, Saleh says.

As a result, the cards issued to all 35,000 Sun employees as part of the project's first phase, which was due to be completed in late June, mainly provide access to the Sun Ray machines, just like the old smart cards.

That access is provided by a conventional contact smart card chip that is inserted into a reader. However, these new cards also have a contactless chip using radio-frequency Mifare technology from Philips Semiconductors. That ultimately will allow cardholders to enter Sun buildings just by waving their cards near readers.

Most Sun buildings use magnetic-stripe cards for building access, and the cards also have a mag-stripe for use during the transition to contactless building access, says Steve Kruschke, new technologies and applications manager, who has led the physical security side of the JavaBadge project.

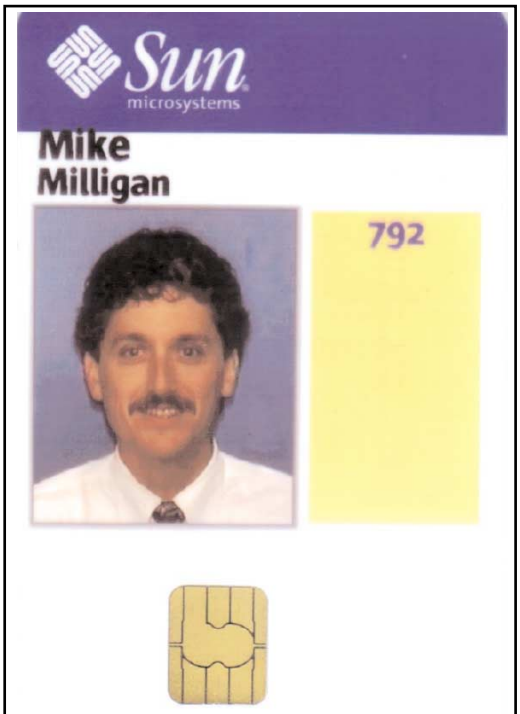
Kruschke says Sun decided to switch to contactless technology for several reasons. For one thing, mag-stripe readers wear out after about 250,000 swipes and have to be replaced periodically, he says. Contactless readers are solid-state devices that have a longer life expectancy. Kruschke says Sun pays $250 to $300 for the contactless readers from InfoGraphics Systems, about the same as it paid for mag-stripe readers.

Sun also wanted a technology that would allow it to write new data to an ID card. For instance, if a woman gets married and changes her last name, Sun can issue a new card with the same ID number – thus not changing its access control database – but with a different name.

Sun has changed over the access control systems at two buildings so far, and plans to switch over an entire campus this summer, Kruschke says. The rest of Sun's buildings will be converted over a few years.

Employees say the card is more convenient, he says. "Just the fact you don't have to line up the card with a reader. You just quickly pass it by the reader. It's a lot easier to use when you've got your briefcase and coffee cup."

But, he says, employees have had to learn that they must take the new JavaBadge with them wherever they go. "People used to use the badge to get in the door and then forget about it. People on occasion have left the badge in the Sun Ray machine and gotten stuck outside the building."



One of Sun's new employee ID cards that secures network access and will be used for contactless building access.

The second phase of the JavaBadge program began this month, and will include use of the smart card to store user name and password combinations that provide Sun employees access to their data from outside of Sun facilities. This will allow Sun to phase out use of the SecurID tokens that generate random numbers for network access.

Ultimately, Saleh says, the smart cards will store PKI-based digital certificates. These are considered more secure than static user name/password combinations because PKI systems require users to respond to a challenge from the network that is different each time, meaning that even if someone copies the response they could not use it to sign on later.

Another feature will be smart card access to an Internet portal tailored to each employee, providing, for instance, memos from that worker's department head.

With Java Card's capability to add new applications after issuance, Saleh says Sun hopes to add other features. One under consideration would allow employees to access their medical records online using the chip card for authentication.

Saleh estimates the budget for the JavaBadge program at no more than $3 million, including two full-time employees from the IT program assigned to the project. <

> US VISIT, Page 1

and Customs Enforcement to track expellees from the country.

Currently, there are 2,000 fingerprint scanners deployed for IDENT and 12 million sets of images in its database. The government will have to add scanners and fortify the capacity of the database that stores biometric data to handle the larger volumes under US VISIT.

While IDENT will be used for now, Homeland Security will put out to bid a contract to develop a new system designed to handle larger volumes. Jim Williams, director of US VISIT, hopes to issue a proposal to systems integrators for this new system by mid-November, with contract submission in January and an award scheduled in May 2004.

Williams said he wants to consult with vendors to make sure that what the government is requesting is realistic. This signals a positive shift from past practice, according to a government official who attended the meeting. "Jim Williams made it clear he wanted to clear away the bureaucratic underbrush and establish new lines of communication with the vendor community," the official says.

The government is not likely to specify how the system should be built. Instead, it will specify the performance metrics it wants met, such as time it should take to process a traveler, and acceptable error rates. "The key will be to address the metrics and adhere to them," says Joseph Atick, president and CEO of biometric vendor Identix Inc., who attended the briefing.

Williams told attendees that Homeland Security would be looking at systems integrators with government experience to manage the US VISIT implementation. Some of the integrators likely on the government's list include Northrop Grumman Corp., BearingPoint Inc., Maximus Inc., EDS and Computer Science Corp., experts say.

An underlying message received by some in attendance was that if vendors want to be involved in US VISIT they would do well to have relationships in place with some of the large systems integrators.

Once Homeland Security awards the contract in May 2004, the integrator will have to hit the ground running because of tight deadlines. By the end of 2004 US VISIT is scheduled to be operational in all seaports and at the 50 busiest land border crossings, with full implementation at all border crossings by the end of 2005. DHS also will expect the systems integrator to be able to make improvements to the system after it is installed.

The US VISIT proposal is not expected to address how Homeland Security will process visitors from the 27 nations whose citizens can enter the United States without visas. Congress has set an October 2004 deadline for those nations, which include major U.S. trading partners, to add biometric data to their passports in order to remain in the Visa Waiver program.

Meanwhile, the State Department took a first step toward putting chips into U.S. passports, issuing a document asking vendors to comment by July 28 on plans to add a contactless smart card chip to passport books. State specified at least 64 kilobytes of memory to store biometric data, double the 32K memory that ICAO set as a minimum.

Atick's overall impression of the meeting was positive. "The take-home message from this is that it's a program that has the attention of the administration at the highest levels," he says. Speaking of Homeland Security Secretary Tom Ridge, Atick says, "Ridge has said that DHS will be judged by the success or failure of this program." <

Consumers Purchase Privacy Protection Products

Some 33.4 million Americans have purchased products to avoid identity theft, check their credit report, or surf or shop online anonymously, according to a survey released last week from the Hackensack, N.J.-based Privacy & American Business. The survey placed the value of the privacy product market around $2.5 billion. Credit check and identity theft protection products range from $69.99 to $119.99 annually and products that allow for anonymous online shopping range from $50 to $100 annually. <

NIST Fingerprint Contest Announced

The National Institute of Standards and Technology will be conducting the Fingerprint Vendor Technology Evaluation this fall, the organization announced last week. The test will evaluate the capability of fingerprint systems to meet requirements for both large-scale and small-scale applications. It will also consist of multiple tests with combinations of fingers, for example, single fingers, two index fingers, four to ten fingers, and different types and qualities of fingerprints. Further details regarding the test are to be released this month. <

County Uses Hand Biometrics

Campbell, Calif.-based IR Recognition Systems, the hand geometry patent holder, announced Monday that Chesterfield County, Virginia, has implemented the company's HandReader to provide off-hours access at the county's administration building. Chesterfield County's existing access control system for the 5-story main administration building, is comprised of keys and the HandReader. Because of the difficulty of retrieving keys from employees there is discussion of deploying more readers, county officials said. <

IDNewswire
Trends in Personal Identification and Biometrics

Editor
Zack Martin
zachary.martin@thomsonmedia.com

Group Editor
Donald Davis
don.davis@thomsonmedia.com

Contributing Editor
Michael Fenner
michael.fenner@thomsonmedia.com

Advertising Sales
Jim Baker
james.baker@thomsonmedia.com

Publisher
Robert Jenisch
robert.jenisch@thomsonmedia.com

Group Publisher
Timothy Murphy
timothy.murphy@thomsonmedia.com

Thomson Media: *Pres. & CEO: James M. Malkin; Pres./CEO Publishing & Conference Group: Bruce Morris; CFO: William Johnston; SVP, Operations: Celie Baussan; CTO: Raymond Ouellette;VP, Business Development and Strategy: Greg Mazzanobile; VP, Human Resources: Robert DeNoia.*

IDNewswire is published biweekly by Thomson Media. Visit our Web site at http://www.cardtechnology.com.

Subscribers who want multiple copies of IDNewswire should contact Barbara Mahin at 212-803-8768 or barbara.mahin@thomsonmedia.com for information. The annual subscription rate is $695. For subscription, renewal or licensing information, please contact Barbara Mahin at 212-803-8768 or barbara.mahin@thomsonmedia.com.

For advertising information, contact Jim Baker at 312-983-6179 or james.baker@thomsonmedia.com. Editorial offices are located at 300 S. Wacker Drive, 18th Floor, Chicago, IL 60606. Telephone: 312-983-6168. FAX: 312-913-1365.

THOMSON™

The Role of Smart Cards as a Privacy-Enabling Technology

The following is from the Smart Card Alliance's SmartTalk teleconference on "Privacy and Secure ID Systems" held on June 26. The following presentation is by Gilles Lisimaque, senior vice president of the business development group, at Gemplus Corp., a major supplier of chip cards.

As locks and keys are one element of the security measures protecting a house, smart cards are the active tools helping to protect the personal information of a cardholder while at the same time enforcing the security rules of the card issuer's application. Smart cards represent a part of a more complex application system and contribute to enforce its overall security.

The smart card contains an embedded computer chip that can be either a microprocessor with internal memory or a memory chip alone. The chip on the card connects to a reader with direct physical contact or with a remote "contactless" electromagnetic interface.

With an embedded microprocessor, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signatures), and interact intelligently with a smart card reader. Smart cards are used worldwide in a variety of applications including financial services, telecommunications, transportation, healthcare, retail, and secure identification in government and corporate environments.
Over 1.75 billion smart cards were shipped worldwide in 2002 (source Eurosmart).

Smart cards, like many other card technologies, can store digital information either in clear text or ciphered formats. They possess a unique ability that set them apart from other identification technologies as they can process information and check credentials before doing anything related to an application. This allows an application to rely on the active action of the card itself to enforce the application rules even when used in an unknown or insecure environment.

The microprocessor can be programmed to only work after the user has been authenticated, in which case the smart card will refuse to process any request or release any information until the legitimate card user agreement is verified (either by presenting a PIN or checking the user's biometric information).

If some user-related information stored in the card should only be released to some authorities, the microprocessor has the ability to check the credentials of the application (or terminal) that asks for this information.

To protect personal information, each smart ID card is designed to act as a personal firewall. The firewall is implemented to ensure that data objects are served from the card only when an external system is authenticated as having predetermined access rights to the data.

The provision of any personal information on the card can be linked to a technique that seeks cardholder permission before information is released. The permission can be a cardholder's PIN, password, or a biometric factor. Only after the smart ID card has verified the PIN, the password, or the cardholder's biometric, can it then release the appropriate information.

It is of course possible to have information in the card "access free" (such as the user's name) and to protect more sensitive information (such as the user's address) with a user identification request (e.g. PIN). Other private user information stored in the card, such as a driver's license number or age may be protected by an even more sophisticated verification of credentials and released only if the application (in the terminal or at the host site) can prove to the smart card it is entitled to access it.

Each time a smart card is enabled, it will ask its user to authenticate himself or herself before the card allows any protected information to be accessed. Only the unprotected (public) information about the cardholder will be available otherwise. Most of the time this unprotected information is the information printed or engraved clearly on the plastic of the card (e.g. first and last name), which can be accessed when the card is presented to a third party.

The information required to identify an individual typically depends on the individual's role in the situation. For example, when stopped by a police officer for a traffic violation, the police officer is entitled to access all information stored on the card related to driving (driver's license information), as well as car insurance. However, the police officer will not have access to unrelated personal information about the cardholder, such as healthcare, even if this information is stored on the same card.

The smart card's ability to process information and react to its environment gives it a unique advantage in providing authenticated information access. Unlike other forms of identification (such as a passive printed driver's license), a smart card does not expose all of an individual's personal information (including potentially irrelevant information) when it is presented.

In the example of a visit to the doctor's office, the same smart card used as a driver's license may also contain personal private health information related to the cardholder (e.g. emergency medical data, blood type, allergies, medical insurance coverage, etc.). When presented to a medical doctor, the smart card will verify the doctor's credentials and release only the required information. Nevertheless, the same card presented to a police officer will not allow him or her to access the private healthcare information of the user. The smart card keeps a very strict separation between unrelated applications

> **Privacy,** Page 7

Smart Card Security Features

- **Tamper-resistance**
- **Extreme difficulty of duplicating or forging cards**
- **Data security, ensuring the privacy, authenticity, and integrity of data encoded on the ID card**
- **Encryption**
- **Digital signatures**
- **Prevention of information-sharing among applications**
- **System challenges, authenticating the components**

> Privacy, Page 6

stored in the same physical card.

This last example shows how the smart card can also answer questions without releasing critical information. As the age of the cardholder is indicated in most drivers' licenses, bars and tobacco shops also use them to check if the cardholder is of legal age. It is easy to program a smart driver's license card to answer to an age request with just the legal information allowing the merchant to comply with the law, but without giving unrelated personal information.

In such an example, the card could answer by giving a digital signature to the bartender certifying the cardholder is old enough, but without giving out the exact birth date. The bartender could store in his own system (or print) a receipt proving he did check the age of his customer, but could not create any kind of user database because the card would not release the user's address, for example, without the explicit consent of the user.

The same mechanism could also be used for older citizens to indicate if they are entitled to senior discounts while still preserving their privacy and not giving away the exact age or any other personal data.

Every smart card system around the world, including ID systems, has implemented similar credential principles. In payment systems, the card releases the user's credit card number and digitally signs the transaction. If the terminal does not have the correct credentials the card may either not operate or will generate a signature that is meaningless for the bogus terminal.

In cellular phones, the cards are used to verify if the user has a valid wireless subscription, but the card will not accept any information to be stored in its memory unless the back-end host on the network has correctly signed the data sent to the card (e.g. short text messages stored in the user's smart card).

For the most robust security and privacy, the secure ID system may require that system components authenticate the legitimacy of other components during the identity verification process. This can include the smart ID card verifying that the automated reader is authentic and the reader in turn authenticates the validity of the smart ID card. The smart ID card can also ensure that the requesting system has established the right to access the information being requested. This creates a trusted chain of elements interacting with each other.

When compared with other tamper-resistant tokens, smart cards currently represent the best trade-off between security and cost. When used in combination with other technologies such as public key cryptography and biometrics and when properly implemented, smart cards are almost impossible to duplicate or forge, and data in the chip cannot be modified without proper authorization (e.g., with passwords, biometric authentication, or cryptographic access keys).

As long as system implementations have an effective security policy and incorporate the necessary security services provided by smart cards, users can have a high degree of confidence in the integrity of their information and its secure, authorized use.

Privacy, authenticity, and integrity of data encoded on ID credentials are primary requirements for a secure ID system. Sensitive data is typically encrypted, both on the smart ID card and during communications with the external reader and system. Digital signatures can be used to ensure data integrity, with multiple signatures required if different authorities created the data. To ensure privacy, applications and data on the ID credential must be designed to prevent information-sharing.

While privacy breaches can still occur with the use of smart cards, the technology features discussed here can significantly prevent fraud, deter counterfeiting, and protect private information.

Because smart cards are programmable, ID systems that incorporate them are flexible. They can be privacy-invasive, privacy-protective, or privacy-neutral, depending on the motivations driving the overall system design. Smart cards do, however, bring unique capabilities that allow them to be the most privacy-protective of any ID token technology.

When on-card matching is used, smart ID cards offer an important privacy benefit – anonymous go/no go support. If the smart ID card is determined to be authentic (enrolled and not revoked, expired, or counterfeit) and the cardholder's identity is verified, the person's identity does not have to be divulged externally.

The identity of the cardholder can be verified by means of a single secure message, sent externally by the smart ID card indicating a correct or incorrect match. The door, terminal equipment, or computer should not be able to record the actual identity of the person being verified. The equipment records only that what was presented was an authenticated smart ID card and that a good or bad credential match resulted.

Verification of cardholder identity is often required at multiple locations. For example, there are multiple locations in an airport that may require security measures for physical access. When multiple checkpoints are necessary, the costs of equipping every check-in desk, security checkpoint, and boarding gate with ID verification technology are a consideration. A smart card-based ID system can be deployed cost-effectively at multiple locations by using small, secure, and low-cost portable readers that take advantage of a smart card's ability to provide offline verification.

Smart cards can provide convenient identity verification. A smart ID card can contain information such as biometric characteristics (one or more as necessary) or other data to assist with the confirmation of the cardholder's identity. In certain situations (such as at unstaffed locations), a smart ID card and suitably equipped reader can verify an individual's identity quickly and efficiently, offering a good balance between security and cardholder convenience.

As in all large IT systems, no one component can be used outside of its context and still perform as intended. Smart cards, having the ability to execute program code in a secure environment, can verify that what they are asked for (e.g. release information) is acceptable according to the security/privacy policy attached to the given information.

If the information is free, it will be released. If the information is to be released only after the cardholder's consent and to a police officer and in a ciphered form, the card will prompt its user for verification, check the credentials of the terminal asking for the information, and only after negotiating a session key will it release the information.

But the card is only a small element of the whole system. As mentioned before, the card should have been issued in a secure manner, the system in which it is used should take care of the information released by the card (transport, storage, backup) and have the same security and privacy rules in all part of its subcomponents. Just as locked doors can only protect a house if the walls are not made of paper and the windows are not left open. <

Also presenting during the SmartTalk conference call were Kent Blossom, director of IBM Safety and Security Solutions; Jeff Katz, vice president of marketing at Atmel; Phil Becker, editor of Digital ID World; and Randy Vanderhoof, executive director of the Smart Card Alliance. For more information about SmartTalk events or the Smart Card Alliance contact Vanderhoof at rvanderhoof@smartcardalliance.org.